No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF OF *AMICUS CURIAE* GESELLSCHAFT FÜR FREIHEITSRECHTE E.V. IN SUPPORT OF RESPONDENT MICROSOFT CORPORATION

OWEN C. PELL
Counsel of Record
SUSAN L. GRACE
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
212-819-8200
opell@whitecase.com

Counsel for Amicus Curiae Gesellschaft Für Freiheitsrechte e.V.

278153

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

QUESTION PRESENTED

Whether 18 U.S.C. § 2703 authorizes a court in the United States to issue a warrant that compels a U.S.-based provider of email services to disclose data stored outside of the United States.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iv

STATEMENT OF INTEREST OF THE *AMICUS CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 6

I. THE CONSTITUTIONAL IMPORTANCE OF THE RIGHT OF DATA PROTECTION IS WELL-ESTABLISHED IN GERMANY AND THE EU 7

A. Constitutional Background in Germany 8

i. The census decision (1983) 8

ii. The decision on online searches (2008) 10

B. Constitutional Background in the EU 12

Page

II. THESE CONSTITUTIONALLY GUARANTEED RIGHTS TO DATA PROTECTION HAVE BEEN IMPLEMENTED AT THE LEGISLATIVE AND ADMINISTRATIVE LEVELS IN GERMANY AND THE EU 13

A. Implementation of Data Privacy in Germany and Its Balancing With Other Important Societal Interests 14

B. Implementation of Data Privacy in the EU and Its Balancing With Other Important Societal Interests 17

III. THE GOALS OF PREVENTING AND PROSECUTING INTERNATIONAL CRIME AND TERRORISM ARE BEST SERVED BY THE USE OF THE MLAT PROCEDURES 18

CONCLUSION 24

TABLE OF AUTHORITIES

Page

CASES

BVerfG[1] *Beschl.* v. *15.12.1983*,
BVerfGE 65 (census decision) 8, 9

BVerfG Beschl. v. *27.2.2008*,
BVerfGE 120 (decision on online searches) . 10, 11, 12

BVerfG Beschl. v. *17.2.2009*,
BVerfGE 122 19

L.H. v. *Latvia*,
European Court of Human Rights,
July 29, 2014 13

S. and Marper v. *The United Kingdom*,
European Court of Human Rights,
Dec. 4, 2008 13

TREATIES AND STATUTES

18 U.S.C. § 2703 7

Basic Law for the Federal Republic of Germany,
available in English language at https://www.
gesetze-im-internet.de/englisch_gg/ ..... *passim*

Charter on Fundamental Rights of the European
Union, Mar. 30, 2010, 2010 O.J. (C83) 389 .... 3, 8, 13

---

1. German Federal Constitutional Court ("Bundesverfassungsgericht," abbr. BVerfG).

Page

Consolidated Version of the Treaty on European Union, May 9, 2008, 2008 O.J. (C115) 4, 13

Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol Numbers 11 and 14, Jun. 1, 2010, C.E.T.S. No. 005 .....3, 8, 13

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal Matters 20

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data 4, 20

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime 21

Page

German Code of Criminal Procedure, available in English language at https://www.gesetze-im-internet.de/englisch_stpo/. 19

German Federal Data Protection Act, available in English language at https://www.gesetze-im-internet.de/englisch_bdsg/ 12, 15, 17

German Money Laundering Act, available at English language at https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Gesetz/GwG_en.h 19

Supplementary Treaty to the Treaty between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, Ger.-U.S., *done* Apr. 18, 2006, T.I.A.S. No. 09-1018.1 ..... *passim*

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)..... *passim*

Treaty on the Functioning of the European Union, Art. 294, Oct. 26 2012, 2012 O.J. (C326) 47 .....4, 8, 13

Page

U.S.-European Union Agreement on Mutual Legal Assistance, *done* Jun. 23, 2003, T.I.A.S. No. 10-201.1 ..... *passim*

OTHER AUTHORITIES

Alexy, *Theorie der Grundrechte* [Theory of Fundamental Rights] (1986) 18

Annual report of the Berlin Data Protection Commissioner 2007, available at https://www.datenschutz-berlin.de/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2007-Web.pdf 14, 16

Annual report of the Berlin Data Protection Commissioner 2008, available at https://datenschutz-berlin.de/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2008-Web.pdf 16

Bavarian Data Commissioner, 89th Conference of federal and state Data Protection Commissioners on Mar. 18 and 19, 2015, Wiesbaden, available at https://www.datenschutz-bayern.de/dsbk-ent/DSK_89-Charlie.html.....19

Court of Justice of the European Union, Press Release No 84/17, 26 July 2017; available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf 22

Page

Hansen, *Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter* [Confidentiality and integrity of data and IT-systems in the age of cloud computing], DuD 2012 (Datenschutz und Datensicherheit) 12

Joint Statement by First Vice-President Timmermans and Commissioner Avramopoulos, available at https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20160414_3_en.....21

Münchener Kommentar zur Strafprozessordnung [Munich Commentary on German Code of Criminal Procedure] (2014).....16

Press Release of the EU Commission, available at: http://europa.eu/rapid/press-release_IP-17-99_en.htm 21

Press Release No. 894/17 and 89/16 of the Court of Justice of the European Union, available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf and https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160089en.pdf.....21

STATEMENT OF INTEREST OF THE *AMICUS CURIAE*[1]

Gesellschaft für Freiheitsrechte e.V. (Society for Civil Rights; "GFF") is a non-partisan German non-profit association with the goal of defending human rights and civil liberties in Germany and Europe. Through strategic litigation GFF advances especially the rights to privacy, freedom of information and of the press against state intrusions and violations. Cases are brought before German courts, supported by a network of NGOs and activist groups, who occasionally act as joint plaintiffs. Several US-based organizations have cooperated with GFF to help establish strategic litigation in human rights as a new tool within the German legal landscape. Organizations like GFF are traditionally critical towards powerful multinational corporations like Microsoft. In this case, however, GFF is supporting Microsoft in the protection of the individual rights of internet users.

As discussed below, in Germany, data protection has been an important issue for decades. To some extent, this derived from the German national experience, which involved bitter lessons of collective experience with dictatorship and widespread government surveillance of individuals. Based on protections created in the German Constitution, decisions by the Federal Constitutional Court of Germany made it clear that citizens have a basic right to self-determination over their personal data

---

1. This brief is filed with the written consent of all parties. No counsel for a party authored this brief in whole or in part, nor did any person or entity, other than *Amicus* or its counsel, make a monetary contribution to the preparation or submission of this brief.

flowing from constitutional guarantees of human dignity and personhood. In 2008, the Federal Constitutional Court articulated a constitutional guarantee of the confidentiality and integrity of IT systems aiming to create a core space where every individual can behave freely.

Limiting the government's power to access personal data, therefore, from a German perspective serves as a guarantor of individual liberty. In times of digital transformation, the privacy of personal data is understood as an integral part of a person's dignity. This point has not only been confirmed, but also outlined and strengthened by German legislation and jurisprudence. As a consequence, infringing someone's personal data has virtually a comparable legal status of a violation of rights as infringing on someone's closest possessions, as both are equally crucial prerequisites for self-determination and, ultimately, liberty itself.

Following the strong connection between human dignity and an individual's personal data (and as e-mails have become a central part of modern private communication), GFF urges this Court not enforce the warrant at issue in this case, which seeks to circumvent European law, and in a German context, would violate German law.

SUMMARY OF ARGUMENT

This case poses the question whether a U.S. court may enforce a warrant requiring Microsoft to produce data stored in the European Union. GFF supports Microsoft in seeking to have enforcement of the warrant denied.

1. In Germany and generally in the EU the right to data protection is a fundamental right incorporated in the German and European Constitutions. In Germany, it is understood as the right to informational self-determination and the right to the confidentiality and integrity of information technology systems which both derive from the general right to privacy contained in Art. 2 para. 1 in conjunction with Art. 1 para. 1 of the German Basic Law. The scope, explicitly determined by the German Federal Constitutional Court, rests on two principles. *First*, on the understanding of an individual as a self-determined human being living in a free society. *Second*, it takes into consideration modern developments in technology which, on the one hand, widen the possibilities of privacy, but at the same time open new ways of breaching privacy, which in turn leads to unpredictable risks to individual liberty. Therefore, it is crucial for individuals to be able to estimate where their data goes and who can access that data. Considering the omnipresence of information technology systems and the rising amount of circulating data and networking systems, the State is required to protect its citizens in order to assure that their data remains confidential. As such, under German (and EU law), when a data subject entrusts his / her data to a service provider, the data subject does not lose their data privacy rights.

2. In the European Constitution, the protection of personal data is covered by Art. 7 and 8 of the Charter of Fundamental Rights of the EU (CFR EU). While Art. 7 provides for the protection of privacy in general, Art. 8 explicitly refers to the protection of personal data. In addition, Art. 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR), which is

binding for the EU according to Art. 6 § 3 of the Treaty on the EU (TEU), encompasses the right to personal data. And according to Article 16 of the Treaty on the Functioning of the European Union (TFEU), everyone has the right to the protection of personal data concerning them.

The EU aims to set a high standard of data protection in all Member States. For this reason, it implemented the General Data Protection Regulation ("GDPR"), which will apply from May 25, 2018 and will regulate questions precisely like the one at issue in order to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. Significantly, the right to informational self-determination and the right to the confidentiality and integrity of information technology systems are not absolute rights. They are limited by competing interests, e.g., where national security is at stake. By way of the principle of proportionality it is to be ensured that national security and data protection as a precondition for a free and democratic society are accomplished at the same time. Taking the principle of proportionality into account, the EU has implemented a Directive which rules the processing of personal data by competent authorities for the purposes of anti-crime and anti-terror measures. This Directive carefully considers the balance between the right to data protection and the need for security.

4. Subject to this condition, an effective fight against crime and terrorism requires also cross-border cooperation. That is why the EU and the United States negotiated the U.S.-European Union Agreement on

Mutual Legal Assistance, *done* Jun. 23, 2003, T.I.A.S. No. 10-201.1 (the "EU MLAT") to ensure their ability to collaborate on the basis of a specific procedure which includes processing data and exchanging information. The same applies to cooperation between Germany and the United Sates, which is assured by the U.S.-Germany Supplementary Treaty to the Treaty between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, Ger.-U.S., *done* Apr. 18, 2006, T.I.A.S. No. 09-1018.1 (the "German MLAT"), which was put in place at the same time as the EU MLAT. Taking into account the fundamental need for protection of personal data, the foreign access to German or European personal data is only conceivable with the restrictions of formalized procedures like those established in the EU and German MLATs.

5. Germany and other European countries have the legal and constitutional obligation to protect their citizens against interferences with rights that have the status of acknowledged human rights regardless from where the interference originates and whether such interference is lawful in the foreign jurisdiction that ordered it. The EU and German MLATs *both* recognize the territorial and jurisdictional interests of the EU and Germany with respect to data privacy, while also providing a way for the United States to lawfully access the information sought under the warrant at issue without enforcing that warrant. Whether by limiting the reach of the SCA or by applying the EU MLAT, this Court should deny enforcement of the warrant in this case.

ARGUMENT

GFF comes before this Court with a perspective that is, perhaps, distinct from the American perspective of data privacy. The understanding of data protection and the importance of this right for German society has developed from first-hand experience with a long and stony path of human rights violations and abusive behavior by the government towards its citizens. During two brutal dictatorships—the Nazi regime from 1933 to 1945 and in this context especially the communist German Democratic Republic (GDR) from 1949 to 1989/90—Germans had to deal with steady governmental surveillance and profound violations of their human rights.

These experiences opened the eyes of the German society to the fact that unlimited government access to personal data can have the gravest consequences for the person concerned and can be the beginning of the end of individual freedom. It was, after all, the registers of residents and punch card systems that enabled the Nazi regime to carry out their genocide with such notoriously cruel efficiency. Germans also experienced the Nazis' systemic surveillance and terror, forcing people to betray their neighbors by informing the secret police ("Gestapo") about any "deviant" behavior or the abode of persecuted individuals, which led to the known horrible consequences.

Having survived the worst, the people of the former East Germany again found themselves in a situation of pain when the communist GDR established another regime of fear based on unlimited government surveillance. Under the communists, homes were tapped, literally millions of individuals were monitored, and lives were destroyed

and even taken. Again the State used neighbors, friends and even family members to spy on its citizens in order to get as much information as possible. For forty years Germans had to fear that their best friends and family were potential informants for the GDR national security agency ("Stasi").

This history has created in German society a strong sense of the need for the protection of individual privacy—even while providing a way for society to protect itself from crime and terrorism. Situations like the Nazi or communist past cannot be allowed to happen again. Privacy protections are now guaranteed by the German Constitution and consistently protected by the jurisdiction of the highest court in Germany, the Federal Constitutional Court of Germany.

Allowing a U.S. court to enforce the warrant at issue under the 1986 Stored Communications Act (18 U.S.C. § 2703) so as to require Microsoft, or any other U.S. company, to produce data hypothetically stored in Germany would force the addressee of that warrant to violate German and European Union (EU) law while also circumventing existing, and sufficiently effective, international treaties that would otherwise fulfill the warrant's objective. Accordingly, the warrant should be quashed.

I. THE CONSTITUTIONAL IMPORTANCE OF THE RIGHT OF DATA PROTECTION IS WELL-ESTABLISHED IN GERMANY AND THE EU.

The right to the protection of personal data occupies an important place in both Germany and the EU. On both

levels, it is enshrined constitutionally. In Germany, the Federal Constitutional Court has explicitly understood the German Basic Law to contain the fundamental rights to informational self-determination and to the confidentiality and integrity of information technology systems, each as specific forms of the general right to privacy contained in the German Basic Law. On an EU level, the ECHR, the CFR EU and the TFEU grant, explicitly or through interpretation, a right to the protection of personal data.

These principles have been confirmed by German Courts in various decisions. Set forth below are certain landmark decisions of the German Federal Constitutional Court in this area.

A. Constitutional Background in Germany.

i. The census decision (1983).

In its census decision handed down in 1983,[2] the German Federal Constitutional Court recognized the right to informational self-determination. It noted that, under the conditions of modern data processing, the protection of individuals against unlimited collection, storage, use and transfer of their personal data is comprised by the general right to privacy contained in Art. 2 para. 1 in conjunction with Art. 1 para. 1 of the German Basic Law.

As the German Federal Constitutional Court points out, the value and dignity of individuals who act as free determined elements in a free society are at the center

2. BVerfG, decision dated December 15, 1983, BVerfGE 65, p.1.

of the German Basic Law.[3] This gains in importance when considering modern developments in technology and the new risks to human personality posed by those developments.

The scope of the right to informational self-determination, expressly set out by the German Federal Constitutional Court, encompasses decisions of individuals with regard to the disclosure and use of their personal data especially concerning the boundaries in which their personal life situations are revealed. As the German Federal Constitutional Court highlights, given the current and future conditions of automatic data processing, the right to informational self-determination requires particularly high protection.[4] Indeed, the Court puts an emphasis on the fact that, nowadays, it is technically possible to store indefinitely and retrieve at any time, in a matter of seconds and without regard to distance, specific information on the personal or material circumstances of individuals (i.e., data subjects) whose identity is known or can be ascertained. Especially if integrated information systems are set up, such information can also be combined with other collections of data to assemble a partially or substantially complete personality profile without giving an adequate opportunity to control the accuracy or the use of this profile to the affected individual. As a result, the possibilities for consultation and manipulation have expanded to a previously unknown extent, which can affect the conduct of each individual, simply because of the mere psychological pressure of public access.

---

3. *Id.*, recital 152.

4. *Id.*, recital 153.

However, if individuals cannot, with sufficient certainty, determine what kind of information about them is known in specific areas of their social environment and, at least to a certain degree, estimate the amount of knowledge a potential interlocutor might possess about them, their freedom to make plans or decisions in a self-determined way can be significantly inhibited. Also, an individual uncertain as to whether "uncommon" behavior is constantly being recorded and the information concerning this behavior is permanently stored, used or transferred to others, will try to avoid standing out through their behavior. This would not only restrict the prospects for the free development of those individuals, but also would be detrimental to the public interest as self-determination is an elementary prerequisite for the functioning of a free democratic society build upon the freedom of action and participation of its citizens.

ii. The decision on online searches (2008).

In 2008, in its decision on online searches,[5] the German Federal Constitutional Court established that the general right to privacy contained in Art. 2 para. 1, in conjunction with Art. 1 para. 1 of the German Basic Law, also encompasses the fundamental right to the confidentiality and integrity of information technology systems.

This decision recognized that recent developments in information technology have led to a situation in which information technology systems are omnipresent and their

5. BVerfG decision dated February 27, 2008, BVerfGE 120, p. 274.

use is central to the lives of many citizens. At the same time, the increasing spread of networked information technology systems entails for the individual new threats to personality.[6] These endangerments emerge from the fact that complex information technology systems such as personal computers open up a broad spectrum of use possibilities, all of which are associated with the creation, processing and storage of data. As a consequence, a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is collected and evaluated by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a profile of that person which the government is then free to store, manipulate and act on.

The risks recognized by the German Federal Constitutional Court are exacerbated in a variety of ways in a networked system, in particular one which is connected to the internet. Above all, the networking of the system opens to third parties a technical access facility which can be used in order to spy on or manipulate data kept on the system. The individual cannot detect such access at all in some cases, or at least can only prevent it to a restricted degree. Information technology systems have now reached such a degree of complexity that the average user cannot afford to protect himself or herself effectively. Also, many possibilities of self-protection—such as encryption or the concealment of sensitive data—are largely ineffective if third parties have been able to infiltrate the system on which the data has been stored.

---

6. *Id.*, recital 177 *et seq.*

Thus, the fundamental right to the confidentiality and integrity of information technology systems recognized under German law protects the interest of the user in ensuring that the data which are created, processed and stored by the information technology system that is covered by its scope of protection remain confidential.[7] Importantly, consistent with the principles discussed above, the German Federal Constitutional Court also explicitly included cloud-based applications in the scope of protection of the fundamental right to the guarantee of the confidentiality and the integrity of information technology systems.[8]

Based on the fundamental nature of privacy rights, the German and European data protection law protect the data subject from losing their privacy rights if they entrust their personal data to service providers. Both, the German law and the European law explicitly address non-public parties, including service providers, which collect or process data from data subjects (so called "Processors") and obliges them to protect the data subject's personal data and their rights on it.[9]

B. Constitutional Background in the EU.

As European law as implemented by the EU is directly applicable to Germany, not only the German Basic Law but

---

7. *Id.*, recital 204.

8. M. Hansen, *Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter,* DuD 2012, p.407 (p.408).

9. Section 1 para. 2, no. 3 of the German Federal Data Protection Act; Article 4 para. 7 and Recitals 1, 27 GDPR.

also European rules determine the basis for the protection of personal data.

The CFR EU grants everyone the right to respect for his or her private life and communications in its Art. 7. The CFR EU also provides for a right to the protection of individual personal data in its Art. 8. Furthermore, pursuant to Article 16 of the TFEU, everyone has the right to the protection of personal data concerning them.

In addition, Article 8 of the ECHR sets out that everyone has the right to respect for his private life and his correspondence. According to consistent case-law of the European Court of Human Rights, the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Art. 8 of the ECHR.[10] The rules of the ECHR are binding for the EU, as Art. 6 para. 3 of the TEU states that the fundamental rights guaranteed by the ECHR constitute general principles of the Union's law.

II. THESE CONSTITUTIONALLY GUARANTEED RIGHTS TO DATA PROTECTION HAVE BEEN IMPLEMENTED AT THE LEGISLATIVE AND ADMINISTRATIVE LEVELS IN GERMANY AND THE EU.

The right to data protection, as guaranteed in the constitutional laws of Germany and the EU, and as

---

10. European Court of Human Rights; *L.H.* v. *Latvia*, July 29, 2014, recital 56; *S. and Marper* v. *The United Kingdom*, Dec. 4, 2008, recital 103.

developed by the respective competent courts, needs to be given effect through implementation. It is at that level that other important, and potentially conflicting, interests must be weighed, especially with respect to preventing and prosecuting international crime and terrorism. Both Germany and the EU have accounted for these important state interests in their data privacy legislation and implementation.

A. Implementation of Data Privacy in Germany and Its Balancing With Other Important Societal Interests.

In Germany, the tension between the protection of personal data and the need to prevent and prosecute international crime and terrorism in order to ensure national security is currently taken into account by the German Federal Data Protection Act, which regulates when personal data may lawfully be processed into the hands of government authorities. In its Section 1 para. 1, the Act expressly states that its purpose is to protect the individual against his/her rights to privacy being impaired through the handling of his/her personal data. This protection also covers the disclosure of information in a case like this one.

With specific regard to a situation like the demand made to Microsoft, the German Federal Ministry of Justice has made an official statement[11] concerning the mutual assistance between U.S. and German law enforcement authorities, and imposes specific procedures

---

11. Statement to be found in annual report of the Berlin Data Protection Commissioner 2007, pp. 188-190.

that allow German data protection law to be reconciled with law enforcement needs.

Indeed, for situations similar to the one at issue—a company obliged through a U.S. warrant to grant access to personal data stored in its establishments in Germany (as opposed to Ireland)—the German Federal Ministry of Justice highlights that, since 2003, the German MLAT has established the approach to be used. German law is clear that absent compliance with the MLAT procedures, it would violate German law for a German company to provide access to personal data stored on its servers in Germany based on a demand from U.S. criminal authorities—including because German law makes clear how companies are to collect and store data in Germany, and that law would not allow a private company storing data in Germany simply to process data to U.S. authorities based only on a U.S. warrant.[12] A company violating these provisions could be fined up to EUR 300,000.00.[13] The German MLAT, however, provides a solution.

Art. 1 para. 5 of the German MLAT provides that a party shall request assistance under the treaty through the competent authorities of the other party, so as to obtain, through the use of compulsory measures or search and seizure, documents, records, and other items located in the territory of the other party and needed in connection with a criminal investigation or proceeding. Thus, the German MLAT expressly establishes that any

---

12. *See*, in this case, especially Section 28 German Federal Data Protection Act.

13. *See* Section 43 para. 2 no. 1 and para. 3 of the German Federal Data Protection Act.

U.S. criminal authority, in the first place, may request personal data via this mutual legal assistance procedure.[14] For that matter, the same procedures would apply to a German criminal authority demanding access to data stored by a private company in the United States. The German criminal authority could not directly oblige the U.S. company to process the data by compelling the U.S. company's German parent company, as the German Code of Criminal Procedure does not provide for such an option. Indeed, such transnational access to data would be considered an interference with the sovereignty of the United States.[15] Any German criminal authority requesting data held by a private company in the United States would have to proceed under the German MLAT.

By highlighting the obligation for U.S. criminal authorities to address themselves first and foremost to the competent German authorities—usually the German Federal Office of Justice—with a concrete request for mutual assistance, the German Federal Ministry of Justice seeks to ensure that German data protection law is respected throughout the MLAT process. Thus, it would be ensured that only the German Federal Office of Justice can instruct the law enforcement authorities in Germany to gather the necessary data in the establishment in question. There would also be a sort of "filter"[16] as, in each case, before providing the data to U.S. authorities

14. *See* annual report of the Berlin Data Protection Commissioner 2007, p. 189.

15. Münchener Kommentar zur Strafprozessordnung/ Hauschild, § 110 Rn. 18.

16. *See* annual report of the Berlin Data Protection Commissioner 2008, p. 147.

the German Federal Office of Justice would have the right to consider any applicable principles of German data protection law that might be presented (for example, the rights of third-parties who are not the subject of inquiry).

From a German law perspective, the German MLAT procedure strikes a reasonable balance between law enforcement on the one hand and constitutional data protection rights on the other hand.

B. Implementation of Data Privacy in the EU and Its Balancing With Other Important Societal Interests.

The EU has taken an approach consistent with German law in implementing data privacy rules that also mitigate the tensions that can arise with national security interests. From May 25, 2018 onwards, the GDPR will be directly applicable throughout all the EU Member States and regulate most aspects of data protection law. The German Federal Data Protection Act will then be reduced to a complementary function. As Art. 1 para. 2 of the GDPR states, the GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Art. 44, *et seq.* of the GDPR creates special rules governing the transfer of personal data to third countries or international organizations (e.g., Interpol). Art. 48 of the GDPR is especially relevant here. It states that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a data controller or processor to transfer or disclose personal data may in principle only be recognized or

enforceable if based on an international agreement, such as the EU or German MLATs.[17]

III. THE GOALS OF PREVENTING AND PROSECUTING INTERNATIONAL CRIME AND TERRORISM ARE BEST SERVED BY THE USE OF THE MLAT PROCEDURES.

As shown above, Germany and Europe are well aware of the potential tensions between data protection and protecting society from crime and terrorism. From a German and European perspective, these conflicts are resolved by striking a balance between these competing interests in a way that allows society to consider the circumstances of individual cases, giving the human right of privacy importance while not neglecting the needs for law-enforcement and national and international actions against crime and terrorism.

Thus, as noted above, the German constitutional right to informational self-determination and privacy is, despite its crucial importance, not an absolute right. It is a right that can be restricted by opposing material interests. However, each interference with a human right must comply with the principle of proportionality.

By requiring proportionality, German law seeks to optimize protected rights.[18] According to this principle, data protection does not have to be an obstacle for security measures. Data protection from a German perspective is an elementary precondition for the functioning of a

17. *See* Art. 48 of the GDPR.

18. *See* Robert Alexy, Theorie der Grundrechte [Theory of Fundamental Rights] (1986), p. 100.

democratic community.[19] But not every regulation that provides security results in a limitation of freedom rights. Indeed, generally speaking, more security may result in more freedom rights because, under secure circumstances, a person can freely develop his/her personality, including by living without fear.[20]

So, data protection is not a "one-way street." But, for the sake of the very same individual freedoms, interferences in data protection must be restricted to the necessary minimum.[21] Serious crimes, like crimes against national defense, crimes against peace, high treason, endangering the democratic state based on the rule of law, treason and endangering external security, crimes against personal liberty and terrorism all are covered by statutory provisions that restrict the fundamental right of data protection and privacy for the benefit of the security of German citizens.

As noted above, European law strives for the same balance. The processing of personal data by competent *authorities* for the purposes of prevention, investigation, detection or prosecution of criminal offences or the

---

19. BVerfG, decision of February 17, 2009, BVerfGE 122, pp. 342 – 374.

20. *See* Bavarian Data Protection Commissioner, 89th Conference of federal and state Data Protection Commissioners on March 18 and 19, 2015, Wiesbaden; available at https://www.datenschutz-bayern.de/dsbk-ent/DSK_89-Charlie.html.

21. *See*, as examples for statutory interference, Sec. 100a para. 1, 100j, 98a of the German Code of Criminal Procedure and Sec. 43 of the German Money Laundering Act, which are only a few of the multitude of statutory provisions that allow prosecutors to collect personal data if it is necessary for the preventions or prosecution of crimes including terrorism.

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security is *not* governed by the GDPR (*see* its Art. 2 para. 2 lit. b)) but by the Directive (EU) 2016/680 (the "Directive").[22] Thus the Directive *protects* on the one hand the citizens' fundamental right to data protection and privacy whenever personal data is used by criminal law enforcement authorities, while at the same time *permitting*, on the other hand, the exchange of data which is essential in the fight against terrorism and cross-border crime.

The Directive also applies not only to the transfer of personal data between and among EU Member States but with third (non-EU) jurisdictions as well, *see* Art. 35, *et seq.* of the Directive. Regarding the transfer of personal data to third jurisdictions Art. 39 of the Directive requires as a legitimate basis for a transnational transfer of personal data, *inter alia*, a bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation, such as the EU and German MLAT. The Directive will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected, while also facilitating cross-border cooperation in the fight against crime and terrorism.[23]

---

22. Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. The Member States shall adopt the Directive by 6 May 2018.

23. *See* Recital 4 of the Directive:

The cooperation principles developed in the MLATs apply to other areas of EU international relations, as well. For example, as shown by recent discussions in Europe and Germany regarding the Passenger Name Record Data ("PNR") agreements[24] between the EU and Canada,[25] as well as EU and U.S.,[26] or the European

---

> The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

24. The PNR Agreement relates to information provided by passengers during the reservation and booking of tickets and when checking in on flights, as well as collected by air carriers for their own commercial purposes. PNR data can be used by law enforcement authorities to fight serious crime and terrorism. As to adoption of the EU Passenger Name Record Directive by the European Parliament - Joint Statement by First Vice-President Timmermans and Commissioner Avramopoulos, available at https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20160414_3_en.

25. Press Release No. 894/17 and 89/16 of the Court of Justice of the European Union, available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf and https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160089en.pdf.

26. Press Release of the EU Commission, available at: http://europa.eu/rapid/press-release_IP-17-99_en.htm.

Data Retention Directive,[27] the pursuit of criminals or national security is not without balance. Rather, a differentiated approach is key to the solution. Depending on the problems presented, different security measures must be taken according to different categories of data (sensitive/personal/anonymized), pursuant to different degrees of suspicion of potentially committed crimes and according to different severities of potential crimes. Further parameters, e.g. the duration of processing and the actuality of data also must be taken into account to do justice to every single case.[28]

It is undeniable that the identification of potential perpetrators is often impossible without processing data and exchanging information between countries. This was the reason for the U.S.-EU MLAT procedures. The idea was to ensure that the United States and Europe could cooperate effectively and efficiently in cross-border criminal investigations and prosecutions with the aim of combatting crime more effectively and in ways that comported with their respective legal systems.[29] By allowing local authorities to monitor and control the release of certain data with regard to European legal

---

27. The Minister of the EU-Member States advises on retention of data (*Vorratsdatenspeicherung*); available at https://netzpolitik.org/2017/diese-woche-minister-der-eu-mitgliedstaaten-beraten-ueber-vorratsdatenspeicherung/.

28. Court of Justice of the European Union, Press Release No 84/17, 26 July 2017; available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf.

29. *See* Agreement on Mutual Legal Assistance between the European Union and the United States of America, *done* Jun. 23, 2003, T.I.A.S. No. 10-201.1.

requirements[30] the MLATs provide the only effective way to correlate the laws of the requested country and the requesting country.[31] On the one hand, the MLATs ensure cooperation between and among MLAT states, and on the other hand, the MLATs exclude one-sided interference by one nation with the territorial sovereignty MLAT states.

As noted above, if U.S. law enforcement authorities circumvented the MLAT as to Germany, that would interfere with German territorial sovereignty. A company located in Germany obliged to transfer personal data based on a foreign warrant would violate German data protection law and would be exposed to high fines. Germany and other European countries have the legal and constitutional obligation to protect their citizens against interferences with rights that have the status of acknowledged human rights, regardless from where the interference originates and whether that interference is lawful in the foreign jurisdiction that ordered it. Germany and other EU Member States would have to protect their citizens against transfers of data which were not permitted under their local laws—just as the United States would act to prevent foreign authorities from breaching U.S. data privacy laws within the territory of the United States.

It is safe to assume that countermeasures against foreign access to European and German personal data may lead to further restrictions of international co-operation for combatting and prosecuting crime and terrorism. This would not only be terribly unfortunate, but would

---

30. *See, e.g.*, Art. 4 para. 6 of the EU MLAT.

31. The MLAT names the requested country and the requesting country "requested party" and "requesting party."

contradict the international approach represented by the EU and German MLATs which balance and reconcile the conflicts of law in this area through international cooperation and established procedures devised and implemented by nation states.

CONCLUSION

For the foregoing reasons, *Amicus Curiae* GFF urges the Court to deny enforcement of the warrant at issue.

Dated: January 18, 2018

Respectfully submitted,

Owen C. Pell
Counsel of Record
Susan L. Grace
White & Case LLP
1221 Avenue of the Americas
New York, New York 10020
212-819-8200
opell@whitecase.com

Counsel for Amicus Curiae
Gesellschaft Für Freiheitsrechte e.V.